BIG BROTHER WATCH

DEFENDING CIVIL LIBERTIES, PROTECTING PRIVACY

Justice Committee: Disclosure of evidence in criminal cases inquiry

Big Brother Watch evidence

June 2018

CONTENTS

About Big Brother Watch

Big Brother Watch is a cross–party, non-party, independent non-profit organisation leading the protection of privacy and civil liberties in the UK. We expose and challenge threats to people's privacy, freedoms and civil liberties at a time of enormous technological change in the UK.

1. Introduction: Digital evidence and disclosure in sexual offences cases

1.1 We welcome the opportunity to submit evidence to the *Disclosure of evidence in criminal cases* inquiry. This submission will focus on digital evidence, disclosure and Article 8 issues in criminal cases, specifically sexual offences cases.

1.2 Digital evidence is unsurprisingly a key part of an increasing number of criminal investigations. Our investigation into police use of digital evidence in November 2017 found that 93% of police forces were extracting data from digital devices including mobile phones, laptops, tablets and computers.[1] The 2015 Angiolini Review into the investigation and prosecution of rape noted that "increased evidential opportunities presented by electronic and digital communication and burgeoning social media has added significantly to the type and volume of material that investigators and prosecutors must consider for evidence and disclosure."[2] Police are also using more and more advanced technology to access, download, and analyse digital evidence as part of these investigations.[3]

1.3 While it is inevitable that the police need to engage with digital information, we are concerned about the extremely intrusive, incoherent and potentially rights-infringing way in which this is currently being done.

1.4 There has been much focus, and rightly so, on the issue of disclosure of digital evidence in sexual offences case, and the Justice Committee's current inquiry has specifically looked at the implications of the growth in volume of digital evidence.[4] However, there has been a disproportionate focus in the media on alleged perpetrators of sexual offences and the potential miscarriages of justice that have occurred or almost occurred to these individuals, supposedly as a result of insufficient disclosure of digital evidence, as opposed to the lack of justice for victims of sexual offences and the digital evidence issues they also face.

---

[1] Big Brother Watch, 'Police Access to Digital Evidence', November 2017 (https://bigbrotherwatch.org.uk/wp-content/uploads/2017/11/Police-Access-to-Digital-Evidence-1.pdf)

[2] Rt Hon Dame Elish Angiolini QC, 'Report of the Independent Review into The Investigation and Prosecution of Rape in London - 'Angiolini Review', 2015, para 20 (https://www.cps.gov.uk/sites/default/files/documents/publications/dame_elish_angiolini_rape_review_2015.pdf)

[2] ACPO, 'ACPO Good Practice Guide for Digital Evidence' March 2012

[3] Privacy International, 'Digital Stop and Search', 27 March 2018 (https://privacyinternational.org/report/1699/digital-stop-and-search-how-uk-police-can-secretly-download-everything-your-mobile)

[4] Disclosure of evidence in criminal cases inquiry: https://www.parliament.uk/business/committees/committees-a-z/commons-select/justice-committee/inquiries/parliament-2017/disclosure-criminal-cases-17-19/

1.5 **We are concerned about the access, collection, analysis, and disclosure of digital evidence in relation to victims of sexual offences, and the potential infringement of victims' Article 8 right to privacy in the disclosure process.**

1.6 This submission considers police and CPS policy and practices in relation to the scrutiny that victims of sexual offences are put under and draws attention to this apparent investigation of victims' digital lives, practices in relation to victims' consent to disclosure of evidence and potential restriction of their Article 8 rights, the use of artificial intelligence to analyse victims' digital evidence, and the lack of expert and sensitive training to deal with the collection and analysis of digital evidence.

Recommendations

1.7 We call on the Government to:

1.7.1 Review police and CPS guidance, policy and practices in relation to the investigation and disclosure of digital evidence, particularly where victims of sexual offences are being re-victimised by indiscriminately intrusive and disproportionate digital investigations, with a view to protecting victims' Article 8 right to privacy;

1.7.2 Review the use of 'Stafford' statements, where victims of sexual offences are encouraged to consent to full disclosure of extremely sensitive and personal details about their private lives which may not be relevant or necessary, and victims may not fully understand what they are consenting to or their other options;

1.7.3 Restrict the use of artificial intelligence or machine-learning systems to access and analyse victims' digital devices; and

1.7.4 Address the lack of expert and sensitive training of police officers dealing with digital evidence.

2. Investigation of victims of sexual offences

2.1 Victims of crime typically supply evidence that is relevant to the crime that has taken place. It is rare that the integrity of such evidence is, by default, put under such scrutiny as it is where victims of rape and sexual offences are concerned. Victims of rape and sexual offences are being re-victimised in the investigation process as the entire contents of their phones and digital devices are accessed and downloaded, and their digital lives and information are subject to intense scrutiny and investigation.

2.2 When a victim reports a crime to the police, and indicates that there is relevant digital evidence on a device, such as a mobile phone, computer or tablet, any and all such relevant devices are taken and sent to an outsourced forensic facility, where a complete copy of all

the information on the device is made. This includes – if present on the device – all texts, emails, pictures, videos, as well as any previously deleted data. Police also request logins and passwords to victims' social media accounts and personal 'cloud' storage services. An average individual's mobile phone can contain the equivalent of 30,000 A4 pages of documents[5] - and will contain a significant amount of extremely personal and sensitive information.

2.3 Once the victim's device or devices is taken by the police for forensic examination, it will not be returned to them until the case is closed.

2.4 Furthermore, the Crown Prosecution Service (CPS) "require police to gather third party material [on victims of sexual offences] from healthcare providers, including psychiatric records, from social services and educational establishments, from counsellors and from family court proceedings. Unless this is done, the CPS will not consider a charge."[6]

2.5 The Angiolini Review also noted that the CPS "consistently reject [case] files due to the absence of key information such as…. social media, and third party material including social services records".[7] There is even a suggestion that the CPS merely do so in order to "[avoid] making decisions and 'buying more time'", and the police themselves have questioned "the need for so much information".[8]

2.6 Dame Vera Baird QC, Policing and Crime Commissioner for Northumbria and the lead for supporting victims for the Association of Police and Crime Commissioners (APCC), has warned:

> *"…we need to ensure that complainants are not discouraged from coming forward to report sexual offences by inappropriate 'fishing' into personal records, access to which is demanded in no other kind of case."* [9]

2.7 Rebecca Hitchen, Policy Officer at Rape Crisis England and Wales, has made clear how victims are made to feel, stating that "the sensation of sex crime survivors is often that they are being put on trial".[10] Sara Thornton, National Police Chief's Council (NPCC) Chair has also cautioned against this intrusive investigation of victims by default:

---

[5] Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)

[6] Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)

[7] 'Angiolini Review', 2015, para 518

[8] 'Angiolini Review', 2015, para 518

[9] Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)

[10] Quoted in The Guardian, 'Police mishandling digital evidence, forensic experts warn', 15th May 2018 (https://www.theguardian.com/law/2018/may/15/police-mishandling-digital-evidence-forensic-experts-warn)

> *"...we must guard against going beyond reasonable lines of inquiry. We cannot allow people to be put off reporting to us because they fear intrusion into their lives and private information that's not relevant to the crime being shared in court."*[11]

2.8 **We are concerned about the extensive amount of extremely sensitive and personal information about a victim which is required by the CPS and gathered by the police by default, without any apparent consideration of the victim's Article 8 right, nor any consideration of the necessity and proportionality of such information to the specific case.**

3. 'Stafford' consent statements & disclosure

3.1 In addition to the amount of extremely sensitive and personal material about a victim which is required by the CPS, victims are being pressured into consenting to the disclosure of all of this material in a way which may prevent due consideration being given to their Article 8 right to privacy, and to an extent of which they may not be fully aware.

3.2 Victims of sexual offences are being encouraged to consent to disclosure of evidence relating to them, including the extensive 'third party material' considered above, by a broad and all-encompassing consent form known as a 'Stafford statement'.[12] This follows from *R (B) v Stafford Crown Court* [2007], which held that in sexual offences cases, a victim's Article 8 right to privacy must be taken into account regarding the disclosure of evidence relating to them, for example psychiatric or medical records, and the victim must be given proper notice and the allowed the opportunity to make representations on the proposed disclosure.[13]

3.3 However, if consent is given via one of these statements, it allows the disclosure of all or any of the potentially extremely sensitive 'third party material' such as psychiatric and educational records, as well as doing away with the requirement for a hearing to consider the victim's Article 8 rights, and preventing the victim from airing their concerns about the disclosure at such a hearing. At the very least, the apparent reluctance of the CPS to consider a charge unless they have available such a broad range of extremely sensitive and personal information appears to be a disproportionate practice which ignores a victim's Article 8 right. Moreover, this practice also puts undue pressure on the victim to consent to the disclosure.

3.4 This practice appears to be at odds with the Attorney General's Guidelines on Disclosure, published in 2013, which make clear that "Disclosure must not be an open-ended trawl of unused material". The guidelines make clear that the defence must indicate which material is relevant:

---

[11] CC Chief Sara Thornton, Police Chief's blog, 11 February 2018 (https://news.npcc.police.uk/releases/police-chiefs-blog-cc-sara-thornton-on-disclosure)

[12] Following *R (B) v Stafford Crown Court* [2007] 1 All ER, a complainant's Article 8 rights must be considered when it comes to disclosure.

[13] This is also now set out in Part 28 of the Criminal Procedure Rules 2010

> "*A critical element to fair and proper disclosure is that the defence play their role to ensure that the prosecution are directed to material which might reasonably be considered capable of undermining the prosecution case or assisting the case for the accused.*"[14]

3.5 The Supplementary Guidelines on Digitally Stored Material further specify, in the context of digital evidence, that "The defence will be expected to play their part in defining the real issues in the case", specifically "defining the scope of the reasonable searches that maybe made of digitally stored material by the investigator to identify material that might reasonably be expected to undermine the prosecution case or assist the defence."[15] The practice of the CPS in both indiscriminately requiring vast amounts of information on victims of sexual offences, and requiring their consent to wholesale disclosure of this material, appears to be in contravention of this official guidance.

3.6 Also concerning is the way that these 'Stafford' statements are presented to the victim as an additional witness statement (indeed, a copy of such a statement seen by Big Brother Watch was marked 'Witness Statement') or a 'consent form', and Dame Vera Baird QC has expressed fears they may not be read thoroughly, resulting in victims unknowingly restricting their ability to exercise their Article 8 rights.[16]

3.7 This is completely at odds with the treatment of the defendant, who is not put under any such obligation to reveal such information or material in relation to their own circumstances, other than to give a 'defence statement'.[17] This was also noted by Rape Crisis England & Wales, who have stated that "There are still huge concerns that someone who reports rape to the police is routinely asked to surrender all of their personal digital data and sign away their right to privacy while a suspected rapist doesn't endure the same level of scrutiny."[18]

---

[14] Attorney General's Office, 'Attorney General's Guidelines on Disclosure' December 2013, para 9 (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf)

[15] Attorney General's Office, 'Attorney General's Guidelines on Disclosure' December 2013, Annex para A3(b) (https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/262994/AG_Disclosure_Guidelines_-_December_2013.pdf)

[16] Dame Vera Baird QC, PCC for Northumbria, 'Letter to Justice Committee', 14 February 2018 (http://www.apccs.police.uk/wp-content/uploads/2016/11/Letter-to-Justice-Committee-Chair-regarding-disclosure-in-criminal-cases-140218.pdf)

[17] Criminal Procedure and Investigations Act 1996, s5(5)

[18] https://www.endviolenceagainstwomen.org.uk/disclosure-crisis-reveals-rape-investigations-are-still-all-about-victim-credibility/

4. Artificial intelligence analysis of victim's digital lives

4.1 Recent reports that police are now trialling the use of artificial intelligence (AI) to trawl through digital evidence, including that of victims of sexual offences, is extremely concerning.[19]

4.2 The police should not be outsourcing such extremely sensitive tasks to an experimental computer system that obstructs accountability and transparency. This could allow for even more disproportionate intrusions of privacy, with the software being trialled by the Metropolitan Police allowing the police to "visualise social networks" and "enable images and videos to be tagged as to whether the content includes…nudity".[20]

5. Out of date policy and guidance

5.1 In addition, we are concerned about the lack of up to date policy in this area, particularly with regards to police practices, and the lack of guidance and safeguards to prevent police from downloading and analysing the entire digital contents of a victim's phone, tablet and laptop, and requiring logins and passwords to personal data storage or 'cloud' services and social media accounts, as a matter of course.[21]

5.2 The most up-to-date policy and 'good practice' guidance available to police to guide their access to digital evidence is the Association of Chief Police Officers (ACPO) *ACPO Good Practice Guide for Digital Evidence* – published in March 2012, over 6 years ago.[22] Meanwhile, the Crown Prosecution Service's *Policy for Prosecuting Cases of Rape* was last updated in 2012.[23] The NPCC and CPS themselves have commented that the two most significant guiding factors in relation to disclosure of evidence, the Criminal Procedures and Investigations Act (CPIA) 1996, and the 2013 Attorney General's Guidelines "were not designed with the sheer volume of digital unused material that is now common to (…) crime cases."[24]

---

[19] https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

[20] https://www.theguardian.com/uk-news/2018/may/27/police-trial-ai-software-to-help-process-mobile-phone-evidence

[21] Angiolini Review, 2015, Para 418, 419, 421 (https://www.cps.gov.uk/sites/default/files/documents/publications/dame_elish_angiolini_rape_review_2015.pdf)

[22] ACPO, 'ACPO Good Practice Guide for Digital Evidence' March 2012 (http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf)

[23] CPS, 'CPS Policy for Prosecuting Cases of Rape', September 2012 (Available: https://www.cps.gov.uk/publication/cps-policy-prosecuting-cases-rape)

[24] NPCC and CPS, 'Written Evidence to the Justice Committee', 24 April 2018 Para 25 (http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/justice-committee/disclosure-of-evidence-in-criminal-cases/written/80778.html)

6. Lack of expert training

6.1 We have further concerns about the lack of expert and sensitive training within the police to deal with the technical aspects of digital evidence.

6.2 Her Majesty's Chief Inspector of Constabulary's (HMIC) 2016 report on the state of policing found that police forces were being "overwhelmed" by digital evidence, and that "forces urgently need to recruit and train a workforce that is fit for a digital future".[25] Another HMIC report in 2015 found that police officers themselves felt "frustrated with their lack of ability to deal with digital investigations".[26]

7. Conclusion

7.1 Not only is it a significant concern that victims of sexual offences are being subjected to such intense and invasive scrutiny of extremely sensitive and personal elements of their lives to the point where they themselves are put under investigation, but that they may not be fully aware of the extent to which they are consenting to disclosure of this information in court, and may even be put under pressure to consent to such disclosure. This invasion of a victim's privacy, through the access to and collection of vast and unnecessary amounts of digital evidence as well as 'third party material', is disproportionate to that experienced by a defendant.

7.2 it would appear that the resulting practices, of access, collection, analysis, and disclosure of evidence, particularly digital evidence, do not allow the victim a fair trial. This has the unsurprising but extremely significant effect that many victims are unwilling to come forward, or withdraw their cases when faced with such intrusion into their private life.

7.3 **Big Brother Watch recommends that the Government urgently reviews current police and CPS practices in relation to the investigation of sexual offences cases, in particular approaches and practices in relation to the collection and examination of victims' digital evidence, and ends the disproportionate intrusion of privacy suffered by victims of sexual offences.**

Griff Ferris

Legal & Policy Officer

[25] HMIC, 'State of Policing 2016, (Published 2017) Pg 24 (https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/state-of-policing-2016.pdf)

[26] HMIC, 'Real Lives, real crimes: a study of digital crime and policing, December 2015, para 5.7 (https://www.justiceinspectorates.gov.uk/hmicfrs/wp-content/uploads/real-lives-real-crimes-a-study-of-digital-crime-and-policing.pdf)